ISSN 2278-3091
Volume 9, No.4, July – August 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse98942020.pdf
https://doi.org/10.30534/ijatcse/2020/98942020

Debit Card Fraud Recognition Using Enhanced Auxiliary Classifier Generative Adversarial Networks

Indrajani Sutedja[1], Ford Lumban Gaol[2], Lili Ayu Wulandhari[3], Edi Abdurachman[4]
[1]Bina Nusantara University, Indonesia, indrajani@binus.ac.id
[2] Bina Nusantara University, Indonesia, fgaol@binus.edu
[3] Bina Nusantara University, Indonesia, lili.wulandhari@binus.ac.id
[4]Bina Nusantara University, Indonesia, edia@binus.ac.id

ABSTRACT

With the recent increasing trend of fraudulent transactions involving debit cards in Indonesia, fraud recognition for debit card transactions is an important and challenging problem to be examined. The purpose of this research is to recognize fraudulent transactions on debit cards with development of the Enhanced Auxiliary Classifier-Generative Adversarial Network (EAC-GAN) model which is a development of Auxiliary Classifier-Generative Adversarial Network (AC-GAN) model. EAC-GAN uses AC-GAN, Synthetic Minority Over-sampling Technique (SMOTE), Principal Component Analysis (PCA), and tuning parameter to recognize fraud transactions in debit cards and increase F1-Score. SMOTE is used to overcome imbalanced data in debit card transactions dataset. Then PCA is required to reduce dimension of the dataset and to know which factors are influential in explaining the phenomenon in the dataset while maintaining characteristics of the data. Parameter tuning is useful to achieve the best F1-Score in training and testing the EAC-GAN model. This research also explores the study of AC-GAN and Convolutional Neural Network 2 Dimension (CNN2D) performance. The result of this research describes that EAC-GAN model beats CNN2D done in the previous research. F1-Score for EAC-GAN is 74% and F1-Score generated by the CNN2D model is 35%. Conclusion from this research is that EAC-GAN model works better in fraud transaction in debit cards surpassing CNN2D model.

Key words: fraud recognition, debit card, Enhanced Auxiliary Classifier Generative Adversarial Networks

1. INTRODUCTION

Now, Bank Indonesia is pushing and promoting cashless transactions by increasing the security and efficiency of the transactions. Some examples of these cashless transactions are balance inquiry, credit card bill payment, electricity bill payment, and cellular credit purchase. Due to this drive, there was a surge of cashless transactions [1] .

There are several types of cards circulating in banks in Indonesia. Some of those are credit cards, debit cards, and ATM cards. A credit card is a means of payment to replace cash in the form of a card that is issued by banks to simplify transactions for customers. The principle of bank credit cards is to lend customers money instead of taking the fund from an account. Different from credit cards, a debit card is an electronic payment card issued by a bank for cash payment substitute. Based on where the debit card was used, there are two types of cards: An Automated Teller Machine (ATM) card and a debit card. Debit cards and ATM cards are special cards issued by banks for account holders which can be used for electronic transactions using his / her account. When the card is used for the transaction, then it would directly deduct the fund available on that account. If it is used for transactions on an ATM, then the card is identified as an ATM card. But if the card was used for cashless payment and shopping using Electronic Data Capture (EDC) machine, then the card is identified as a debit card [1].

Fraud in the context of banking transactions is a common term for every illegal action characterized with deception, concealment, or breach of trust. These actions could be done with or without violent threats or physical force. Generally, fraud can be done by an individual, a group or an organization to acquire money, property or services; to avoid payment or damages incurred from service; or to gain personal or business profit [1]. Fraud is also any sort of attempt that can be devised or attempted by someone to gain profit from others by using dishonest means which would result in the other individual being deceived and suffered financial loss Thus, fraud covers an array of illegal practices and illegal actions that involves fraud being done intentionally or unintentionally.

With the rapid surge of debit card use, fraud involving debit cards also increases [2]. Fraud affects serious loss to the banking industry. Some cases of fraud that have been reported to banks are a case that has caused the loss of around IDR 500.000.000 for 115 customers and one customer of a bank reported a loss of money in his account. Quoting at the twitter. It was reported that the missing fund reached IDR 80.000.000.

From the data above, it can be concluded that fraud has affected tremendous financial deficit, loss of data, and reputational destruction for the majority corporations [2]. For example, fraud in France has caused a loss of £469.900.000. That represents the 4,3% increase in financial losses. Another example in Indonesia, the total loss of a well-known private bank in the country from January to December 2015 due to fraudulent transactions involving debit cards is IDR 36.763.933.064 (97,99%) of total frauds that occurred in that bank). The most frequent types of fraud in that bank are card trapping, card loss, hypnotism, skimming, internet banking, and mobile banking [3]. Card trapping and skimming places on top of the amount and percentage of loss.

Several researches that has been done in fraud detection on debit cards or credit cards have used Convolutional Neural Networks and the obtained F1-Score is between 0.30 to 0.35 [17]. Then Hidden Markov Model (HMMs) and its accuracy reached 80% using combined data between actual data and synthesized data [4]. Next, there is a research using frequency (t-side) analysis, k-Nearest Neighbor (k-NN), and HMMs. The result for t-side is having F = 0.85, k-NN having F = 0.21, and HMMs having F = 0.84 [5] . Then there is also a research using Quick Response Code (QR-code) and pin, but the QR-code is easily scanned. The next research uses Chip and Personal Identification Number (PIN), but Chip and PIN have a weakness [6], but the previous researches are often difficult to implement to detect fraud transactions on debit cards in Indonesia, where the data is imbalanced and the similarity between fraud and non-fraud transactions [7].

Based on a crucial need of fraud detection, this research suggests a detection technique using AC-GAN model to achieve more accurate results [8],[9].

The main purpose of this paper is to increase F1-Score and accuracy, also overcome the imbalanced of data classification using competitive learning algorithm in which there are many ways for detection issues in debit cards that has not yet been fully developed in previous researches because this problem is rarely encountered in developed nations. To achieve this objective, the researcher explores AC-GAN model to solve the classification of imbalanced binary data. The classification itself consists of two classes: fraud and non-fraud transactions. First, the previous research suggested CNN2D as classifier. This research suggests EAC-GAN model. Second, for reduction of data dimension, the first study applies PCA. Then, this study utilizes convolutional layer stacks, Rectified Linear Unit, and collections

2. LITERATURE REVIEW

2.1 *Auxiliary Classifier – Generative Adversarial Network (AC-GAN)*

The framework of GAN (figure 1) is aligned with the game theory: minmax two-player game [10]. To obtain intuition from GAN, we take a simple illustration that represents how GAN works. For example, a police as the first player and a counterfeiter as the second player. The police must learn the differences between a real bill and a counterfeit bill while the counterfeiter tries to make counterfeit bills as like a real bill as possible. In the first stage, the counterfeiter gives real bills and counterfeit bills that are combined and randomized then handing it to the police. The police then differentiate between real bills and counterfeit bills and gives hints to the counterfeiter what makes counterfeits look real. These clues are signal for the counterfeiters to improve the quality of the counterfeits. Next, the counterfeiters get back to the police with improved counterfeits to get the next hints. This process happens continuously so that each player has their best abilities: the police with their ability to differentiate counterfeit bills and the counterfeiter with the ability to produce counterfeits.

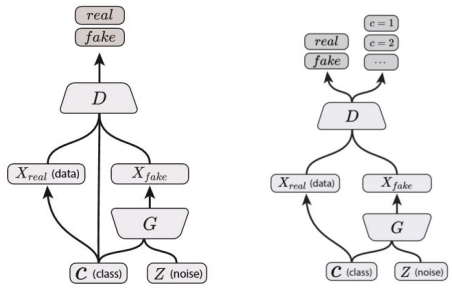

Figure 1: (a) General Architecture of the GAN Model and (b) the AC-GAN Model [11]

Formula for the lost function of GAN can be written as follows [12],[13]:

$$L = E[\log P(S=\text{real} \mid X_{real})] + E[\log P(S=\text{fake} \mid X_{fake})] \quad (1)$$

Where P (S | X) is the probability distribution for the source, X which is an input. Input could be trained data or synthesized data.

These are the formulas used in AC-GAN [17]:

$$L_S = E[\log P(S = \text{real} \mid X_{real})] + E[\log P(S=\text{fake} \mid X_{fake})] \quad (2)$$

$$L_C = E[\log P(C = c \mid X_{real})] + E[\log P(C=c \mid X_{fake})] \quad (3)$$

Where Ls is the correct source and Lc is the correct class. AC-GAN trains model D to maximize LS + LC and trains model G to maximize LC-LS.

2.2 Convolutional Neural Networks

CNN are a class of neural network models with standard structures. The CNN architecture is comprised of the following layers: Convolutional layer, Non-linearity, Pooling layer, and Fully connected layer.

A sample of the CNN architecture is presented in Figure 2.

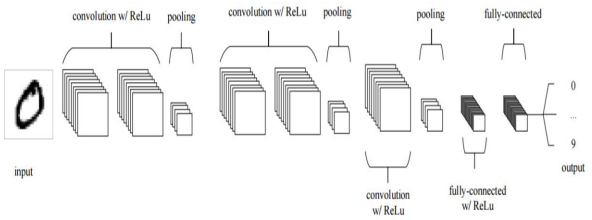

Figure 2: General Configuration of a CNN Model [15]

The objective function L, of the CNN model training, is formulated as follows:

$$L = \frac{1}{2}\sum_{i=1}^{b}\sum_{j=1}^{b_i}(t_{ij} - o_{ij})^2 \quad (4)$$

where: t_{ij} is the actual class of the j^{th} sample of the i^{th} training batch and o_{ij} is the predicted class of the j^{th} sample of the i^{th} training batch.

2.3 Convolutional Neural Network 1 Dimension (CNN1D)

CNN is a mathematical operation that represents signal processing in a linear fashion and time variance [15]. Convolution can be divided into 1D Convolutional, 2D Convolutional and 3D Convolutional. 1D convolutional calculation can be illustrated as follows:

Illustration of a manual calculation in a Convolutional process can be observed in the following figures:

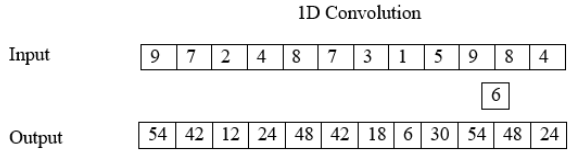

Figure 3: Example 1D Convolution-1

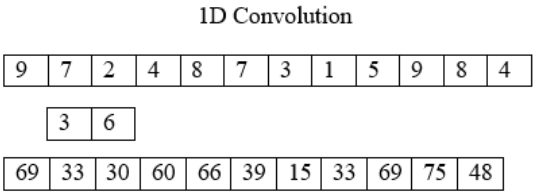

Figure 4: Example 1D Convolution-2

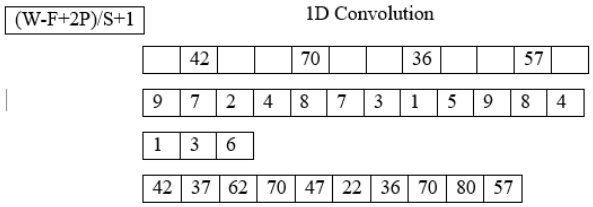

Figure 5: Example 1D Convolution-3

(W-F+2P)/S + 1 (5)

Where: W = weight
F = filter
P = padding
S = stride

3. METHODS

3.1 Research Framework

The research process blocks of this study are represented in the following diagram (Figure 6).

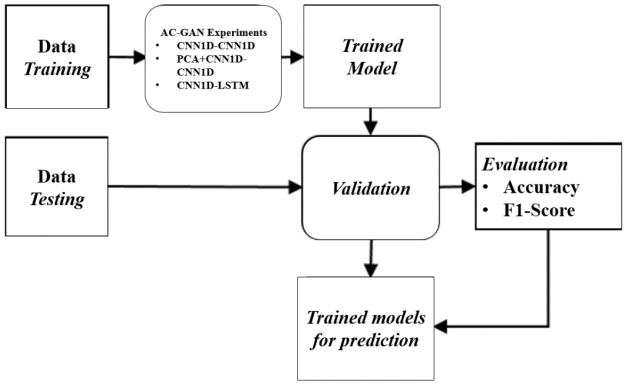

Figure 6: Research Framework

3.2 Dataset

Data collection is a process to extract data by running a query on Bank XYZ's data warehouse, with prior approval from the management of the bank. The data consists of fraud and non-fraud debit card transactions performed through ATM and EDC. Each transaction uses a debit card which contains information regarding [15]:

1. Debit cardholder profile which contains variables such as Card Number, Birthdate, Gender, Customer Type, etc.
2. Transaction entity which contains variables such as Amount Transaction, Date Transaction, and Time Transaction.
3. ATM Entity which contains variables such as WSID, ATM location, and Machine-Id.

The result of early observation of the dataset for this research shows that the dataset is imbalanced [14]. In this case, the amount of data for fraud transactions is way smaller than non-fraud transactions. On top of that, transaction variables for fraud and non-fraud transactions have a lot of similarities so manually, it is very difficult to discern between fraud and non-fraud transactions.

The summary of acquired data from period 2016-2017 for this research is as follows:

Table 1: Dataset

No.	Flag	Rows	Ratio
1	0 = Non-Fraud	13,405	0.977
2	1 = Fraud	9,278	0.022
3	Total	22,683	1.000

3.3 Data Preprocessing

Early data processing involves several processes to transform data from its original format to the format suited for the research's training model. The purpose of pre-processing data is to make data to gather the prerequisites of quantitative analysis. Thus, data handling in this study involves these activities [16], [17]:

1. Data composite estimates such as the frequency and total accumulation from each sample debit card transaction and the transaction amount likelihood group from the past 12 months.
2. Non-numeric data quantification which translates non-numeric data into numeric data.

4. RESULTS AND DISCUSSIONS

On the first stage, the models used are CNN and AC-GAN that are unmodified. Due to multicollinearity in debit card transactions dataset, during modification of the AC-GAN model, one of the developed models had PCA added.

From testing results with package mctest in R, then it was acquired whether that feature have multicollinearity or not.

All Individual Multicollinearity Diagnostics Result

	VIF	TOL	Wi	Fi	Leamer	CVIF	**Klein**	IND1	IND2
avg2_ke_1	Inf	0	Inf	Inf	0	Inf	**1**		1
avg2_ke_2	Inf	0	Inf	Inf	0	Inf	**1**		1

If Klein parameter = 1 then it is multicollinear. From the performed experiment, all features coming from the average values of the total value of the transactions are multicollinear.

4.1 Training and Validation

Training-validation data distribution used in this research is a technique in which 75 percent of the dataset is used to develop the model and 25 percent of the data set intended for testing. Precision and F1 are used as the classifier's performance metrics which are formulated as follows:

$$accuracy = \frac{TF+TN}{total\ testing\ dataset} \quad (6)$$

$$F = \frac{2 \times TP}{2 \times TP + FP + FN} \quad (7)$$

Where
TF: both predicted and actual are fraud.
TN: both predicted and actual are non-fraud.
FP: predicted as fraud but is non-fraud.
FP: predicted as non-fraud but is fraud.

The modification was done in the AC-GAN model which is a contribution and consists of:
1. Modification of model on Generator
2. Modification of model on Discriminator

Table 2: Modification of AC-GAN Model

No.	Modification of AC-GAN Model	Generator	Discriminator
1	EAC-GAN 1	CNN1D	CNN1D
2	EAC-GAN 2	PCA and CNN1D	CNN1D

Validation is done on data with a percentage of 75:25. Model validation serves to measure how good can a trained model make a prediction on data classification from new data (data testing) which was not used in the model training process. Accuracy is a measurement of a model's performance is used for two main reasons: (1) accuracy is more intuitive compared to other metrics such as F1, and (2) accuracy calculations are relatively simpler compared to other metrics.

Table 3: Summary of AC-GAN Model Differences

No.	Modification of AC-GAN Model	Unmodified AC-GAN	EAC-GAN 1 Modification of 1 Generator (CNN1D) and Discriminator (CNN1D	EAC-GAN 2 Modification of 2 SMOTE + PCA + Generator (CNN1D) and Discriminator (CNN1D)
1	Generator Model	**CNN2D**	**CNN1D**	**CNN1D**
2	Discriminator Model	**CNN2D**	**CNN1D**	**CNN1D**
3	Generator Layer	**8**	**8**	**6**
4	Discriminator Layer	**7**	**11**	**11**
5	Dataset	***Image***	***Text File***	***Text File***
6	PCA	X	X	**√**
7	Up Sampling	√	√	√
8	SMOTE	X	√	√
9	Activation Function Generator	Relu → 3 **Tanh** →1	Relu → 3 **Sigmoid** → 1	Relu → 3 **Sigmoid** → 1
10	Activation Function Discriminator	Fake → Sigmoid Aux → **Softmax**	Fake →Sigmoid Aux →**Sigmoid**	Fake →Sigmoid Aux →**Sigmoid**
11	Optimization	**Adam**	**SGD**	**SGD**
12	Architecture Model	-	Figure 6	Figure 7
13	F1-Score	0.3639	0.4515	**0.7460**

4.2 EAC-GAN 1

Modification of 1 Generator (CNN1D) and Discriminator (CNN1D)

EAC-GAN 1 (figure 7) uses CNN1D for generator and discriminator model, 8 layers in generator, and 11 layers in discriminator. It also uses 3 Relu and 1 Sigmoid as activation

function. For optimization, it uses Stochastic Gradient Descent (SGD).

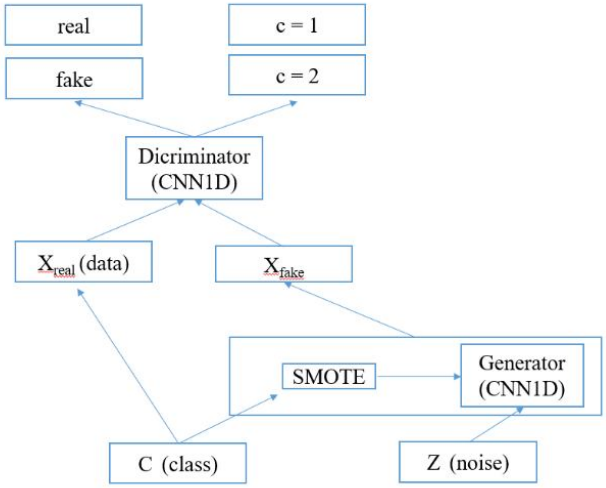

Figure 7: EAC-GAN 1 Modification of 1 Generator (CNN1D) and Discriminator (CNN1D)

Generally, unmodified and modified AC-GAN are the same, the difference is in the modified one, there are SMOTE and CNN1D, a different amount of layers, an active function and different optimizers as seen on Table 3. Summary of AC-GAN Model Differences

4.3 EAC-GAN 2

Modification of 2 SMOTE + PCA + Generator (CNN1D) and Discriminator (CNN1D)

EAC-GAN 2 uses CNN1D for generator and discriminator model, 6 layers in generator, and 11 layers in discriminator. It also uses 3 Relu and 1 Sigmoid as activation function. For optimization, it uses Stochastic gradient descent (SGD).

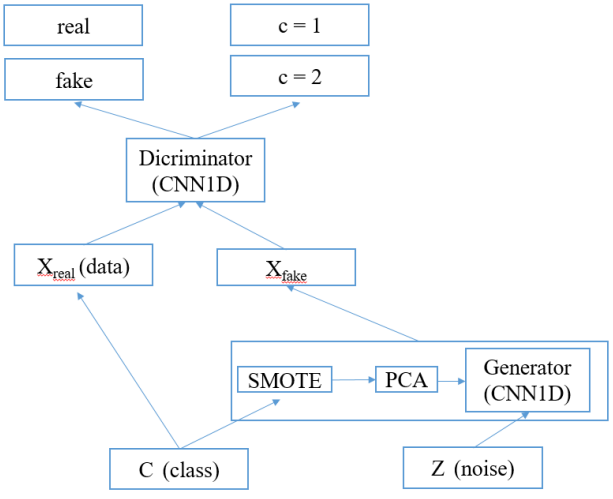

Figure 8: EAC-GAN 2 Modification of 2 SMOTE + PCA + Generator (CNN1D) and Discriminator (CNN1D)

Generally, unmodified and modified AC-GAN are the same, the difference is the modified one has SMOTE and PCA and CNN1D, different number of layers, an active function and different optimizer as seen on Table 3. Summary of AC-GAN Model Differences

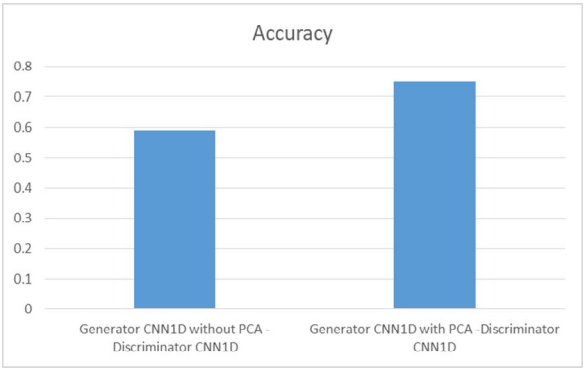

Figure 9: Accuracy Result

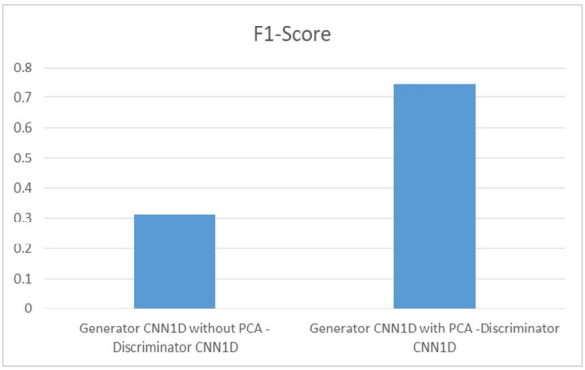

Figure 10: F1-Score Result

The highest accuracy was generated by the AC-GAN model with the CNN1D generator that was added by PCA and CNN1D discriminator, which was 75%. For the highest F1-score, it was generated from AC-GAN with CNN1D generator added with PCA and CNN1D discriminator, which is 74%. But the time required for 50 epochs is 4:50:23. While the fastest time was recorded by AC-GAN with CNN1D generator without PCA and CNN1D discriminator, which is 0:22:15 for 50 epochs. But the resulting accuracy was only 58% and the F1-Score was 31%.

5. CONCLUSION

In this paper, we introduced fraud method detection on debit cards with EAC-GAN. The experiment result from debit card transaction data of a commercial bank shows that our suggested method performs better than the previous one, which is CNN2D. The result according to the performed training and testing, EAC-GAN produces F1-Score 74% over CNN2D F1-Score. Besides that, the generated dataset

generated during this research is primary data of fraud transactions with debit card.

Recommendations from this research are the generation of fraud transactions on debit cards' primary data can be developed further with other features and modification of AC-GAN can be developed further considering the accuracy and F1-Score has yet to reach maximum. The development can be done along with other deep learning models.

ACKNOWLEDGEMENT

Part of this work is assisted by the respective reviewers. The writers also thank the reviewers for their positive feedback and suggestions, which have enhanced the presentation.

REFERENCES

1. Kanika, Jimmy Singla. **Online Banking Fraud Detection System: A Review**, *IJATCSE*, Vol. 8, No.3, pp. 959-962, 2019 https://doi.org/10.30534/ijatcse/2019/96832019
2. A. Singh and A. Jain, **Adaptive Credit Card Fraud Detection Techniques Based on Feature Selection Method**, *Adv. Comput. Commun. Comput. Sci.*, no. May, pp. 437–446, 2019.
3. P. R. Vardhani, Y. I. Priyadarshini, and Y. Narasimhulu, **CNN Data Mining Algorithm for Detecting Credit Card Fraud P.**, *Soft Comput. Med. Bioinforma.*, p. 139, 2019.
4. W. Y. Lai, K. K. Kuok, S. Gato-trinidad, and K. X. Ling, **A Study on Sequential K-Nearest Neighbor (SKNN) Imputation for Treating Missing Rainfall Da,** *IJATCSE*, vol. 8, no. 3, pp. 363–368, 2019. https://doi.org/10.30534/ijatcse/2019/05832019
5. S. Allen *et al.*, **Design Choices for Central Bank Digital Currency: Policy and Technical Considerations**, 2020.
6. D. Singh, R. Ruhl, and H. Samuel, **Attack Tree for Modelling Unauthorized EMV Card Transactions at POS Terminals.**, in *ICISSP*, 2018, pp. 494–502.
7. S. KS and A. Danti, **Online fake review identification based on decision rules**, *IJATCSE*, vol. 8, no. 2, pp. 140–143, 2019. https://doi.org/10.30534/ijatcse/2019/07822019
8. C. L. Chin, Y. L. Lin, and Y. C. Liu, **Various Types Fracture Labeling in Bone Radiographs Using Modified AC-GAN**, *Proc. - 2019 Int. Conf. Technol. Appl. Artif. Intell. TAAI 2019*, no. 1, 2019.
9. J. L. Qiu and W. Y. Zhao, **Data Encoding Visualization Based Cognitive Emotion Recognition with AC-GAN Applied for Denoising**, *Proc. 2018 IEEE 17th Int. Conf. Cogn. Informatics Cogn. Comput. ICCI*CC 2018*, pp. 222–227.
10. I. J. Goodfellow, J. Pouget-abadie, M. Mirza, B. Xu, and D. Warde-farley, **Generative Adversarial Nets**, *Adv. Neural Inf. Process. Syst.*, pp. 2672–2680, 2014.
11. A. Odena, C. Olah, and J. Shlens, **Conditional Image Synthesis With Auxiliary Classifier GANs**, *IICLR 2017*, pp. 1–16, 2017.
12. E. Wu, H. Cui, and R. E. Welsch, **Dual Autoencoders Generative Adversarial Network for Imbalanced Classification Problem**, *IEEE Access*, vol. 8, pp. 91265–91275, 2020.
13. X. Xie *et al.*, **Generative Adversarial Network-Based Credit Card Fraud Detection**, *Commun. Signal Process. Syst.*, no. September 2019, pp. 1007–1014, 2020. https://doi.org/10.1007/978-981-13-6508-9_122
14. U. Fiore, A. De Santis, F. Perla, P. Zanetti, and F. Palmieri, **Using generative adversarial networks for improving classification effectiveness in credit card fraud detection**, *Information Science*, vol. 479, pp. 448–455, 2019.
15. I. Sutedja, Y. Heryadi, L. A. Wulandhari, and B. Abbas, **Imbalanced Data Classification Using Auxiliary Classifier Generative Adversarial Networks**, *IJATCSE*, vol. 9, no. April, pp. 1068–1075, 2020. https://doi.org/10.30534/ijatcse/2020/26922020
16. I. B. K. Manuaba, I. Sutedja, and R. Bahana, **The evaluation of supervised classifier models to develop a machine learning API for predicting cardiovascular disease risk**, *ICIC Express Lett.*, vol. 14, no. 3, pp. 219–226, 2020.
17. S. Wang, G. Liu, Z. Li, S. Xuan, C. Yan, and C. Jiang, **Credit Card Fraud Detection Using Capsule Network**, *IEEE Int. Conf. Syst. Man, Cybern.*, 2018, pp. 3679–3684, 2018. https://doi.org/10.1109/SMC.2018.00622